



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 24 November 2003

Current Nationwide Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The U.S. Department of Energy (DOE) asked for applications from energy firms for matching government funds to develop new nuclear power plants that could be ordered and licensed in the next decade. (See item [1](#))
- The Department of Homeland Security has issued a statement on possible threats against U.S. interests during the Muslim holiday, Ramadan, and the upcoming holiday season. (See item [24](#))
- The Department of State has issued a travel warning recommending that U.S. citizens defer non-essential travel to Turkey. (See item [25](#))

DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *November 22, Reuters* — U.S. and private sector plan pushes new nuke power plants. The U.S. Department of Energy (DOE) on Friday, November 21, asked for applications from energy firms for matching government funds to develop new nuclear power plants that could be ordered and licensed by early in the next decade. Expanding nuclear power use in the United States was a key recommendation of the Bush administration's national energy plan

to meet growing electricity demand while reducing greenhouse gas emissions by depending less on coal as a power plant fuel. **Under the DOE's initiative, the government will match industry investments over the next several years to demonstrate regulatory processes that can make new nuclear power plants more efficient and predictable.** For this latest phase of the department's program, the government will seek proposals from teams led by U.S. power generating companies to develop and implement plans to license and build new plants. "This phase of the program could lead to licensing and construction of the first new nuclear plant in this country since the 1970s," said Secretary of Energy Spencer Abraham.

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_11_21_eng-reuters_pma_US-PRI-VATE-SECTOR-PLAN-PUSHES-NEW-NUKE-POWER-PLANTS&SMContentSet=0

2. *November 21, Reuters* — **New England okays power transmission upgrade plan. New England's electricity grid operator said it approved a regional transmission expansion plan to enhance the reliability of the region's power system over the next 10 years.** ISO New England's plan includes about 250 proposed transmission upgrades that would cost between about \$1.5 billion and \$3 billion depending on which projects were ultimately built. "New England's electric generating capacity has grown by almost a third since the wholesale markets opened in 1999, however, our transmission system hasn't made the same progress and is inadequate in many areas," said Gordon van Welie, ISO New England's president and chief executive, in a statement released on Thursday, November 20. ISO New England operates the power grid and the \$4.5 billion wholesale marketplace for more than 14 million people in Massachusetts, Connecticut, Rhode Island, Vermont, New Hampshire and Maine. **The greatest needs for upgrades are in southwest Connecticut, northwest Vermont and the greater Boston, MA, area and on an east-to-west 345,000 volt transmission path from Massachusetts to Rhode Island to Connecticut.**

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_11_21_eng-reuters_pma_NEW-ENGLAND-OKAYS-POWER-TRANSMISSION-UPGRADE-PLAN&SMContentSet=0

[\[Return to top\]](#)

Chemical Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

3. *November 20, Washington Post* — **Army cites burdens posed by rotation. Army leaders warned on Thursday, November 20, that plans to replace U.S. forces in Iraq early next year with a new wave of troops will present enormous logistical burdens, posing a challenge unlike any military authorities have confronted in recent decades.** "To my knowledge, the Army has never had a rotation like this in the past," Les Brownlee, the Army's acting secretary, told the Senate Armed Services Committee. **On top of dealing with tens of thousands of returning troops, Army authorities are bracing for months of preparing**

nearly as many soldiers slated to go next, many of them reservists who have greater requirements for training, equipment, housing and medical care. All in all, Brownlee noted, more than 120,000 reservists as well as elements from eight of the Army's 10 active-duty combat divisions will be on the move in the first four months of next year, either into or out of Iraq or Afghanistan. Counting active-duty troops, the number in transition will total 200,000 to 250,000, he said. To accommodate the flux, Army officials are developing a day-by-day schedule showing which troops are expected to be where, and when.

Source: http://www.washingtonpost.com/wp-dyn/articles/A63484-2003Nov_19.html

[[Return to top](#)]

Banking and Finance Sector

4. *November 21, The Register (UK)* — **UK ID theft gang jailed for £350K fraud. Six British men were sentenced on Friday, November 21, to a combined total of 15 and a half years imprisonment for involvement in a major ID theft and fraud conspiracy.** The fraud, which netted the gangs £350,000 over two years, is thought to be the biggest case of its kind to date in the UK. **The men used false identities obtained on the Internet to open bank accounts, obtain credit card and apply for loans and overdrafts. Through this subterfuge they obtained £315,000 from Lloyds TSB and a total of £30,000 from the Halifax and Cooperative banks.** The National Hi-Tech Crime Unit reports that the men used "sophisticated techniques to obtain false identities over the Internet." The six used information from a mortgage auction site to obtain the details of people who had recently died. They then applied for accounts in the names of these people, while simultaneously applying to redirect mail to addresses where the fraudsters could pick up 'ghost mail' and 'confirm' fraudulent applications.

Source: <http://www.theregister.co.uk/content/55/34138.html>

5. *November 20, Houston Chronicle (TX)* — **Wells Fargo warning of identity theft risk.** Wells Fargo & Co. customers with personal lines of credit and overdraft protection on their checking accounts are at risk of having their identities stolen. **The San Francisco, CA-based bank mailed letters this week to 200,000 customers whose names, addresses, Social Security numbers and line-of-credit account numbers were in a computer stolen from the office of a consultant hired by Wells Fargo.** "No passwords or personal identification numbers were included in the files. No other Wells Fargo accounts or any other accounts you may have were affected," states the letter signed by Scott Gable, senior vice president of Wells Fargo's Personal Credit Management Group. **As of Thursday, November 20, the bank had no evidence the information had been misused by the thief.** To minimize the chances of the theft expanding, Wells Fargo has taken several steps to re-secure the compromised data. It is changing all the stolen credit line account numbers by the end of the month. It is also paying for each affected customer to have a one-year membership in PrivacyGuard, a credit monitoring service that lets its members know when there is any activity in their credit bureau files.

Source: <http://www.chron.com/cs/CDA/ssistory.mpl/business/2239272>

[[Return to top](#)]

Transportation Sector

6. *November 21, Associated Press* — **Threatening note causes plane to land. A plane bound for London returned to Kennedy Airport early Friday, September 21, after a flight attendant found a threatening note on a seat in the aircraft, authorities said.** Virgin Atlantic Flight 10 departed from Kennedy Airport shortly after midnight Friday but returned at about 1:30 a.m., said Darrin Kayser, a spokesman for the federal Transportation Security Administration. **Kayser said he did not have information about the contents of the note or whether any arrests were made.** He said the FBI was investigating; a message left for the FBI was not immediately returned. **More than 250 passengers aboard the plane were evacuated and rescreened,** Kayser said. The Port Authority of New York and New Jersey conducted a search of the aircraft using canine units, according to Port Authority spokesman Tony Ciavolella. Virgin Atlantic said in a statement that "as Virgin expected, the threat is now viewed as a hoax." The airline said it was cooperating with authorities in the investigation. Source: <http://www.cnn.com/2003/US/Northeast/11/21/plane.threat.ap/>
7. *November 20, Government Executive Magazine* — **Coordinating cargo security rules a challenge. New rules requiring the transportation industry to give the government advance notice of all cargo shipments will require better coordination among the Department of Homeland Security agencies, according to Secretary Tom Ridge.** The new regulations, which go into effect in 15 days, require transportation companies to submit electronic information on all cargo to the Customs and Border Protection (CBP) agency within hours before its arrival at U.S. borders or departure from the country. The length of time that companies have to give notice varies depending on the mode of transportation and whether cargo is outbound or inbound. **To make the rules work, Homeland Security agencies will need to step up their efforts to use each other's information systems, Ridge said. For example, CBP hopes to tap into TSA's Known Shipper Program, which maintains data on frequent cargo carriers.** All cargo information collected by CBP — whether from another government agency or from industry — will be put into a database that is controlled by Homeland Security and linked to other law enforcement and commercial databases. Under the new rules, suspect cargo will be inspected on scene by customs inspectors. Source: <http://www.govexec.com/dailyfed/1103/112003c1.htm>

[[Return to top](#)]

Postal and Shipping Sector

8. *November 21, Associated Press* — **UPS announces 2004 rate increases. United Parcel Service (UPS) said Friday it will raise its ground shipping rates 1.9 percent effective January 5.** The rate increase for the ground shipping rate is lower than in previous years (3.9 percent in 2003, 3.5 percent in 2002). Company officials said this smaller increase has been balanced by increases in other areas, as UPS seeks to recover costs for deliveries both far away and to uncommon delivery areas. The new rates include a dollar delivery charge for commercial shipments headed for remote ZIP codes. There also are increases on the company's C.O.D. and Saturday pickup charges. Mark Davis, an analyst with Cleveland-based FTN Midwest Research, said the new rates do reflect a move on the part of the company to better compete

against rival DHL. The rates, combined with UPS's integrated delivery network, also will put "a lot of pressure" on FedEx, which has established separate networks for its delivery services. "There's kind of a land grab going on here," Davis said. "They're trying to get as much business as they can with the most advanced network. **In addition, UPS will increase its U.S. air and worldwide express service rates by an average of 2.9 percent and the fee for residential deliveries will rise by a quarter, to \$1.40.**

Source: <http://www.miami.com/mld/miamiherald/business/7319777.htm>

[[Return to top](#)]

Agriculture Sector

9. *November 21, Sydney Morning Herald* — **Microchips and satellites, quarantine of the future. Australian livestock in remote areas could one day be implanted with microchips to detect serious diseases such as foot and mouth and Japanese encephalitis, warning quarantine officers via satellite.** That's the long-term vision of researchers at the new Australian Biosecurity Co-operative Research Center (AB-CRC) to be launched in Brisbane Friday by Science Minister Peter McGauran. Center chief executive officer Stephen Prowse said the chips would also be able to detect an animal's physiological condition, giving graziers information on their stock's health status. "You might have an animal that has a chip or a number of chips implanted under the skin and potentially the information could be transmitted by satellite to a detection center," Prowse said. **"We're talking a pretty long-term vision here, 10 or 20 years."** In the meantime, researchers are working on developing hand-held computer devices that graziers will be able to use to monitor and report disease outbreaks in their stock. Prowse said the devices would be designed to relay diagnostic information via the internet to a government veterinarian who could take immediate action to contain a disease outbreak. **At the moment, Prowse said some remote farms were never checked for serious infectious diseases despite the increased risk through the movement of people and animals and the possibility of bioterrorism.**

Source: <http://www.smh.com.au/articles/2003/11/21/1069027299749.html>

10. *November 21, Associated Press* — **Oyster harvest likely to be Maryland's worst.** Preliminary results of a state survey show what Maryland oystermen have suspected since they started scraping the Chesapeake's reefs last month, the oyster harvest this season is likely to be the state's worst ever. **Oyster harvesters set a record low with last year's catch of 53,000 bushels over the six-month season. This year, they are set to pull in less than half that amount, said Chris Judy, shellfish program director at the Maryland Department of Natural Resources (DNR). DNR's survey found about 50 oyster boats in Maryland's part of the bay. The survey estimated 70 harvesters worked the boats, down from 437 harvesters last year and 2,500 in 1999.** "You find some, but you can't make a day's work out of it," said Larry Simns, president of the Maryland Watermen's Association. The season opened October 1 and ends March 31, but "for a lot of people, the season is over now. The legal-sized oysters are in such low quantities, they can't make a living," Judy said. The survey, which aims to assess how well oysters are surviving and reproducing in the bay, offers more bad news for watermen. **Dermo, one of two diseases ravaging Chesapeake oysters, was not significantly knocked down by the year's heavy rainfall, Judy said.**

Source: <http://www.dailytimesonline.com/news/stories/20031121/localnews/679592.html>

11. *November 21, Australian* — **Wild dog parasite infecting cattle.** A parasite spread by dingoes and wild dogs is costing the Australian beef industry an estimated \$30 million a year because it is causing cows to miscarry. **Many of the Australia's beef cattle are believed to have been infected by the neospora caninum parasite by eating grass contaminated with dog feces.** Authorities insist the meat of infected animals is safe for human consumption. The results of a Queensland government study on the parasite were presented Wednesday to the International Society of Veterinary Epidemiology and Economics in Chile. **Of almost 6000 beef cattle tested in western Queensland, 15 percent were infected with neospora. Of 32 properties surveyed, only one showed no indication of the infection. The study showed infected cows had three times the abortion risk of uninfected animals.** Calves born to infected cows have a 90 percent of chance of having the parasite themselves. Natural Resources Department land protection officer Melissa Derrick said dogs became infected after eating fetal tissue or afterbirth, and passed the parasite eggs in feces.
Source: http://www.theaustralian.news.com.au/common/story_page/0,574,4,7927204%255E30417,00.html

[[Return to top](#)]

Food Sector

12. *November 21, New York Times* — **U.S. considers food labels with whole–package data.** The Food and Drug Administration (FDA) said Thursday that it was considering whether to **require food companies to list nutrition information in its entirety, rather than by serving size, on packaged–food labels.** Currently, if a package contains more than one serving, consumers must multiply nutrition data by the number of servings to determine total calories, fat, and carbohydrates. Some consumer groups and nutritionists have argued that such food labels are misleading and could cause consumers to take in more calories, sodium, and fat than they realize. The potential change in the composition of food labels, was among the topics that FDA officials and representatives from the food industry discussed Thursday at a workshop the agency held to explore any links between obesity, food labels, and packaging. **The FDA has been looking at ways to improve food labels since August, when Mark B. McClellan, the head of the agency, commissioned a task force to come up with ways to help address obesity. The committee is expected to issue its suggestions in February.**
Source: <http://www.nytimes.com/2003/11/21/business/21food.html>
13. *November 20, Ag Professional* — **USDA: New food safety research agenda.** The U.S. Department of Agriculture (USDA) has announced a unified food safety research agenda to improve the efficiency and effectiveness of food safety programs. **The research agenda is one of several key initiatives USDA is implementing to enhance food safety and improve food inspection systems.** USDA also released a list of additional research needs specific to meat, poultry, and egg products that the Food Safety and Inspection Service will encourage non–governmental entities to address. **The new agenda includes research to investigate the ecology, epidemiology, virulence, and genetic characteristics related to pathogenicity for E. coli O157:H7, Salmonella, Listeria monocytogenes, and other foodborne pathogens to identify targeted control measures.** Research will also develop effective farm, feedlot, transportation, handling, and other pre–processing intervention strategies for reducing the

incidence and levels of antibiotic resistant microorganisms and key foodborne pathogens in meat, poultry, eggs, and fresh produce. **Additionally USDA will develop, validate, and transfer technology of new and improved processing methods to reduce or eliminate key foodborne pathogens.**

Source: http://www.agprofessional.com/show_story.php?id=22371

[\[Return to top\]](#)

Water Sector

14. *November 21, Tampa Tribune* — **Water department mishandled test result. The Hillsborough County, FL, Water Department mishandled a positive E. coli bacteria test result taken in October and is now notifying south county customers by mail. Officials said Thursday that they are reviewing procedures to avoid a repeat of the problem.**

During the past year, the department has had four incidents of bacteria levels testing too high at scattered sites. Retests have come back negative, and officials say they don't think the problem is a health risk. Every month, the county tests at 120 sites in each of the department's two service areas, which divide 170,000 customers into northwest and south-central sections. In the most recent case, one site had a positive result. Three times in the past year, tests have come back positive for coliform bacteria, a sign that potentially dangerous elements could be in the water. This was the first positive for E. coli. The test results mean some people, infants, the elderly, and those with compromised immune systems, might be at increased risk for illness.

Source: <http://news.tbo.com/news/MGAINX8X9ND.html>

[\[Return to top\]](#)

Public Health Sector

15. *November 21, Reuters* — **Bacteria samples stolen. Brazilian authorities urged residents of Rio de Janeiro on Friday to be careful after lab samples of cholera and typhoid fever were stolen with a biologist's car. Doctors and police in the Brazilian city said the bacteria had been securely packed and represented no risk if not opened, but acknowledged the samples could be dangerous if removed from the package.** Silvio Valle, a biosecurity expert with the government's Fiocruz research institute, graded the biohazard of the stolen material as two on a scale of four in televised comments, asking viewers to contact Fiocruz immediately if they found the box of samples. A Fiocruz biologist was taking the samples to a conference in a neighboring state when she was carjacked at gun point on Thursday night. Police said they found the stolen car in the early hours on Friday inside a shantytown, but without the samples in it. Still, they said the criminals had obviously been after the car and did not know about the bacteria. Armed robberies are frequent in Rio de Janeiro.

Source: http://news.yahoo.com/news?tmpl=story2&cid=573&u=/nm/20031121/od_nm/crime_brazil_bacteria_dc&printer=1

16. *November 20, BBC News* — **Test for early detection of SARS.** Scientists say they have developed a new test for the virus that causes Severe Acute Respiratory Syndrome (SARS) which could lead to earlier detection of the disease. **The procedure, developed by the**

National Taiwan University, produces results in two to three days. Other tests which look for antibodies produced by the body to fight the Corona Virus can take much longer. The earlier a case of Sars is detected, the less chance there is that a patient will spread the disease to others. The new test picks up substances called antigens which are produced by the virus. These are the compounds which trigger the body's immune system to produce antibodies. Many of the other tests for SARS developed last winter only work once the antibodies have been produced. **They have also developed a new method to collect specimens from patients' saliva by rinsing the mouth with water. This means that healthworkers can reduce their chances of catching the SARS virus because they do not have to get close to the patient to carry out a throat swab to collect saliva for the tests.**

Source: <http://news.bbc.co.uk/1/hi/health/3222834.stm>

[[Return to top](#)]

Government Sector

17. *November 21, Government Computer News* — **Homeland's ICE gains CIO, seeks name change. Gary Hartwig, a career Customs Service official, has become interim CIO of the Homeland Security Department's Immigration and Customs Enforcement (ICE) arm. Officials at the homeland agency also are working to change its name to Investigations and Criminal Enforcement.** Hartwig started as ICE's first CIO October 24, an agency spokesman said. From March 1 until his recent appointment, he was director of ICE's executive information division. Previously, he had been the Customs Service's director of administration, planning and policy in the Office of Investigations. **Officials said the change in the agency's name to Investigations and Criminal Enforcement arose because most ICE employees have criminal investigation functions.** They include employees of the Federal Protective Service, the government's air marshals, the homeland department's immigration detention and removal activities, the Air and Marine Operations division that inherited Customs' air and sea enforcement mission, and operations to stem child pornography and financial crimes. ICE executives are seeking final approval of the name change now, officials said.

Source: http://www.gcn.com/vol1_no1/daily-updates/24258-1.html

18. *November 20, Congress Daily* — **A House Homeland Security panel has approved a bill to revamp first responder grant funding programs. The bill (H.R. 3266) would replace the Department of Homeland Security's current programs for distributing grant funding to localities and states with a new initiative to allocate money based on threats, vulnerabilities and risk assessments rather than other factors such as population.** The Emergency Preparedness and Response Subcommittee approved the bill by voice vote, and the full committee is expected to take up the measure during next year's session. "The legislation before us today is a bold new model for distributing federal grant funds to first responders based on building essential capabilities across the country to meet the threats and vulnerabilities communities face from terrorism," said full committee ranking Democrat Rep. Jim Turner of Texas. It also requires the department's science and technology division to establish national standards for first responder equipment six months after enactment of the bill. The standards must specifically address thermal imaging, radiation detection, chemical detection and interoperability equipment, among other items.

Source: <http://www.govexec.com/dailyfed/1103/112003markup1.htm>

[\[Return to top\]](#)

Emergency Services Sector

Nothing to report.

[\[Return to top\]](#)

Information and Telecommunications Sector

19. *November 22, Associated Press* — **EU sets up Internet security agency.** The European Union (EU) governments agreed Thursday, November 20, to launch an agency to protect the Internet by alerting the public about computer viruses, identity theft and other crimes committed online. **The European Network and Information Security Agency is to be operational in early 2004. It is to help governments, businesses and consumers protect their computer systems and data** and inject some order in the varying approaches EU nations have taken so far to combat Internet crimes. "Trust and security are crucial components in the information society," Erkki Liikanen, the EU's information society commissioner, said in a statement.

Source: http://seattlepi.nwsourc.com/business/aptech_story.asp?category=1700&slug=EU%20Online%20Security

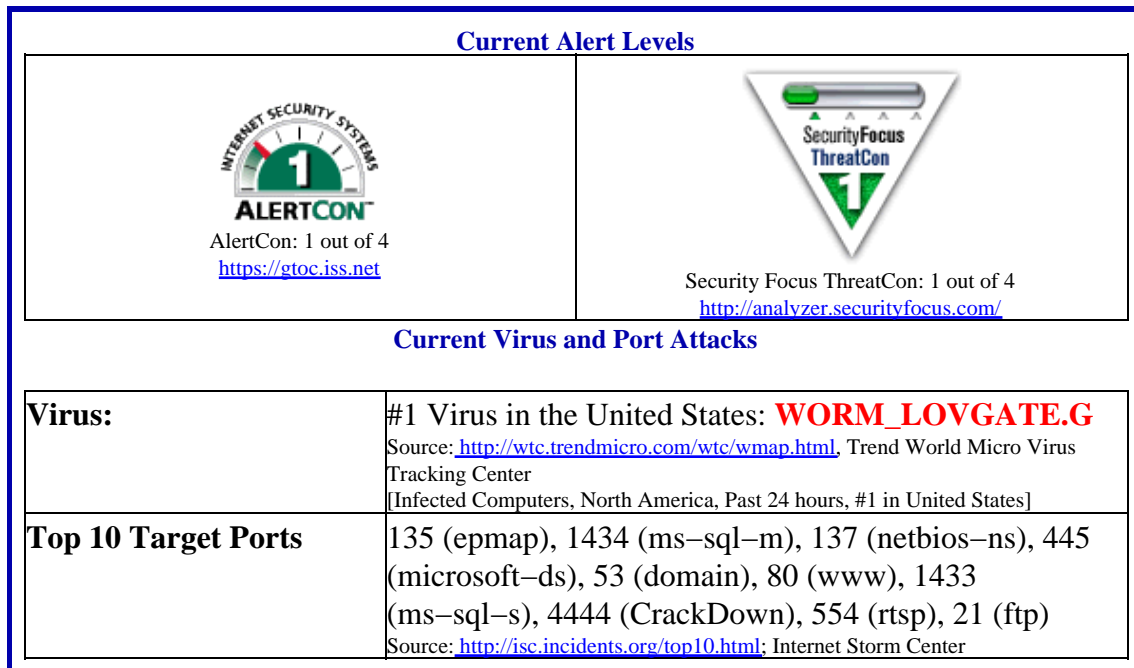
20. *November 21, eWEEK* — **Debian Linux under attack by hackers. An unknown cracker compromised several machines belonging to the Debian Project, including servers that house the project's bug-tracking system and security components.** Officials from the project said last week they are working to restore all of the affected machines. Debian is an open-source operating system that uses the Linux kernel and also includes a number of packages and tools from the GNU Project. **This is the second such attack against an open-source project in recent weeks.** Someone tried to insert a backdoor into the Linux kernel two weeks ago.

Source: <http://www.eweek.com/article2/0.4149.1394325.00.asp>

21. *November 20, Macworld.co.uk* — **Apple releases security patches. Apple Computer Inc. has released security updates for Mac OS X Panther 10.3.1 client and server systems and Mac OS X Jaguar 10.2.8 client and server operating systems.** The Panther update includes the following updated components: OpenSSLzlib "gzprintf()" function, an update to the open-source lossless compression library used by Darwin, the kernel of Apple's OS. The Jaguar update improves a number of components, including document formatting system, groff; Unix macro processor component, gm4; and Mail w/CRAM-MD5 authentication (used to debug common authentication services). It also improves OpenSSL (a robust, commercial-grade, full-featured, and open-source toolkit with a general-purpose cryptography library that implements the Secure Sockets Layer); Personal File Sharing; QuickTime for Java; and the zlib "gzprintf()" function. Both updates are available for download from Apple's Website: <http://www.info.apple.com/support/downloads.html>

Source: http://www.infoworld.com/article/03/11/20/HNapplepatch_1.html

Internet Alert Dashboard



[\[Return to top\]](#)

General Sector

22. *November 23, Washington Post* — **Private cargo plane in Iraq hit by missile. A pair of suicide car bombers attacked police stations in two towns north of Baghdad on Saturday, November 22, killing 11 policemen and five civilians** in an escalating campaign against Iraqis cooperating with the U.S.-led occupation. **Insurgents also hit a DHL cargo plane with a surface-to-air missile as it took off from Baghdad's international airport**, military officials said. The plane's left wing gave off smoke as the craft returned to the runway safely. There were no injuries. After the incident, Royal Jordanian Airlines, the only company offering commercial service to Baghdad, canceled its flights from Amman. In the northern city of Mosul, assailants shot and killed an Iraqi police colonel who was in charge of a force protecting oil installations. **Attacks on Iraqis in government, police forces, paramilitary units and pro-American political parties have grown in number and ferocity in recent weeks.** On Thursday in the northern city of Kirkuk, 95 miles southwest of Mosul, a suicide bomber in a pickup truck detonated at the local offices of the Patriotic Union of Kurdistan, killing five bystanders. In Baghdad on Friday, insurgents fired rockets at two hotels housing foreigners and at the Oil Ministry building. No one was killed in the assaults.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A5467-2003Nov2 2.html>

23. *November 22, Associated Press* — **Military units join Georgia opposition.** Some military units began to join tens of thousands of opposition protesters dancing and singing in the streets of Georgia's capital Sunday, November 23, as support for President Eduard Shevardnadze waned. **Saturday the opposition broke into parliament and took it over, saying the November 2 elections that chose the new body were rigged. Nino Burdzhnaze proclaimed herself acting president** until early elections in 45 days. The elections, which the

United States also criticized as fraudulent, became a tipping point for a population fed up with the poverty, corruption and crime that have dogged Georgia for more than a decade. **Russia and the United States both fear instability in the ex-Soviet republic, strategically located on the borders of Russia and Turkey, between the oil-rich Caspian Sea and the ports of the Black Sea.** Russia has military units stationed in Georgia. U.S. troops are also in the country on a counter-terrorism mission, training Georgian forces to uproot Islamic insurgents from neighboring Chechnya who take refuge in Georgia's mountainous terrain.

Source: http://www.usatoday.com/news/world/2003-11-22-georgia-protests_x.htm

24. *November 21, Department of Homeland Security* — **Statement by the Department of Homeland Security on continued al Qaeda threats.** In the wake of the recent terrorist bombings overseas, the Department of Homeland Security (DHS) has been aggressively monitoring and assessing information with other Federal agencies and state and local partners on potential terrorist threats to the United States. The U.S. Intelligence Community continues to receive and evaluate a high volume of reporting indicating possible threats against U.S. interests during the Muslim holiday, Ramadan, and the upcoming holiday season. This reporting, combined with recent terrorist attacks, has created an atmosphere of concern in which increased vigilance here at home is prudent and may be key to deterring or disrupting terrorist attacks. **The DHS remains concerned about al Qaeda's continued interest in aviation including using cargo jets to carry out attacks on critical infrastructure as well as targeting liquid natural gas, chemical and other hazardous materials facilities.** In response to this information, the DHS, the Federal Bureau of Investigation and the Terrorist Threat Integration Center have issued an advisory to security personnel intended to increase the awareness of appropriate state and local authorities and the private sector responsible for security of critical infrastructure and other potential target sets. Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0300.xml

25. *November 20, U.S. Department of State* — **Travel Warning: Turkey.** The Department of State recommends U.S. citizens defer non-essential travel to Turkey. On November 15, two synagogues in Istanbul were the targets of suicide car bombs. On November 20, the British Consulate General and the London-based HSBC bank in Istanbul were damaged by powerful explosions, killing dozens and wounding hundreds. **These incidents represent a significant change from prior attacks in Turkey, which have previously involved small-scale, random bombings and small numbers of casualties.** Terrorist actions may include, but are not limited to, suicide operations, hijackings, bombings, or kidnappings. Terrorists do not distinguish between official and civilian targets. **Increased security at official U.S. facilities has led terrorists and their sympathizers to seek softer targets** such as public transportation, residential areas, clubs, restaurants, places of worship, hotels, schools, outdoor recreation events, resorts and beaches. Source: http://travel.state.gov/turkey_warning.html

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-6631

Subscription and Distribution Information: Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202-323-3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.